

Curriculum Vitae

Dave Kleiman CCE, CEECS, CIFI, CISSP, DFCP, MVP
 4371 Northlake Blvd #314,
 Palm Beach Gardens, FL 33410
dave@davekleiman.com • 561.310.8801
<http://www.ComputerForensicsLLC.com>

**Summary of Experience**

Dave Kleiman specializes in computer forensic examinations, electronic discovery, data recovery, and incident response, and has more than 22 years of security focused information technology experience. He has analyzed hundreds of cases including cases involving enterprise technologies such as Windows Server, Microsoft Exchange, Microsoft SQL, Microsoft SharePoint, and Microsoft Dynamics GP. Dave has testified at many trials and depositions in civil and criminal matters, rendering expert opinions regarding computer-related data and operations in Federal, State, and Military courts as a computer forensics expert and has served as a court appointed neutral expert. His testimony and analysis has included computer, cell-phone, email, network, and internet analysis, evaluating electronic discovery plans, evidence spoliation, intellectual property, trademark/patent infringement, insurance claims, fraud, business reorganization, and breach of contract. Dave has an extensive list of computer security and forensic certifications, he is one of less than 100 Microsoft Enterprise Security MVPs in the world, and he developed a Windows Enterprise operating system lockdown tool. Dave has made appearances on national news television as a subject matter expert in computer forensics. He has been published in more than ten books including The Official CHFI Exam Study Guide for Computer Hacking Forensics Investigators, and has created many tools, tricks, and tips for time saving forensic techniques that he presents in labs at national security and cybercrime conferences.

Dave has held the positions of the VP of Information Technology for Intelliswitch, Inc., an International Voice over IP Company and Internet Service Provider. The Chief Information Security Officer for Securit-e-Doc, Inc. a security software development company. The Director of Information Technology for Suffolk Construction, a national commercial construction company with more than a billion in annual revenues. A Florida Certified Law Enforcement Officer for the Palm Beach County Sheriff's Office with more than three thousand employees, he also served as a Systems Analyst during his tenure at PBSO.

Dave has performed the following services for former employers and clients including but not limited to Law Enforcement Agencies, Florida State Attorneys' Offices, Federal Public Defender's Office, Department of the Navy, Naval Criminal Investigative Service, and Law Firms.

- Perform forensic examinations, electronic discovery services and respond to critical computer security incidents by collecting, preserving, recovering, analyzing, filtering, and searching digital evidence/artifacts such as electronic mail extraction, and database examinations
- Conduct advanced computer and network forensic investigation functions relating to various forms of electronic fraud, identity theft, computer intrusion, theft of intellectual property, denial of service, and financial fraud investigations
- Identify legal need for discovery and provided methods of electronic discovery and litigation support
- Prepare for court appearances and depositions for criminal and civil testimony
- Perform analysis of expert witness reports and testimony
- Create policies and procedures regarding response to computer crime events, regulatory compliance issues, and operational/investigatory processes. Understand the legal and technological impact such a policy will have on an organization, and the consequences faced by an organization when such a policy does not exist
- Execute risk assessments, security audits, and ensure agency compliance with information security best practices
- Conduct research, analysis, and services designed to detect and deter instances of system and network exploitation
- Ensure that all incidents and resolutions are recorded and tracked to meet audit and legal requirements and to incorporate resolutions for future security incidents
- Lead meetings, divide responsibilities, and influence people to take action to assist in the resolution of security incidents
- Provide executive and organizational briefing at conclusion of incident with cause and effect
- Develop and foster long-term liaison contacts with cyber security organizations
- Develop and maintain secure regional networks
- Conducted business continuity exercises with emergency action plans
- Develop forensic courseware; provide supporting seminars and labs
- Developed a Windows Operating System lockdown tool, S-Lok, which surpasses Microsoft Common Criteria Guidelines

Computer Expert Witness Experience

U.S. vs. Corporal Jeremy Garcia (U.S. Navy Southern Judicial Circuit, 17MAY11-SEKB-0103-8DMA)-2012-10-16
Expert Witness for the Department of the Navy - Testimony encompassing mobile devices, cell phones, and the various tools and techniques for retrieving data from mobile devices. How the progression of cell phone tools and their firmware and software updates have affected the ability to access physical cell phones and their associated files systems, and decode and analyze that data. The advancement of chip-off forensics and how data can be retrieved when other methods are unavailable or fail.

Platypus Wear, Inc., et al., vs. Horizonte LTDA, et al. (U.S. District Court Southern District of Florida, Miami, Case No. 08-CV-20738-KMM Moore/Torres)-2012-06-(25-26)

Expert Witness for Plaintiffs - Intellectual Property Trademark Infringement - Testimony encompassing spoliation of electronically stored evidence, explaining how data is overwritten and the methods to and possibilities of recovering that data. Detailing how and when large data files were written to a Microsoft Windows Servers hard drives after an order was granted on motion to compel production of electronic data storage device for forensic examination. Demonstrating how thousands of keyword search results were found in the unallocated space of the hard drives and how that deleted data was retrieved and presented for privilege review.

Raymond F Kravis Center vs. Lexington Insurance Company, et al. (15th Judicial Circuit Palm Beach County, Florida, Case No. 502005CA002274XXXXMB - Fine/Brown)-2012-03-22

Appointed Co-Neutral Expert - Insurance Claim - Testimony detailing the development of a two-phase Electronic Discovery plan for the court and qualifying why the various steps in each phase were necessary on a Custom SQL Database Server, Microsoft Exchange Server, Files Server, Backup File Server, Retired Server, 3 years of Backup Tapes, User Computer Systems, and User Server Shares. Discussing with plaintiff's and defendant's experts, issues of burdensomeness, timeliness, and comments /objections to each step of the phases. Insuring the plaintiff and defendant understood and could carry out the finalized steps of e-discovery.

PWI, et al., vs. Horizonte Fabricacao Distribuicao Importacao E Exportacao LTDA, et al. (U.S. District Court Southern District of Florida, Miami, Case No. 08-CV-20738-AJ Jordan/McAliley and Case No. 07-CV-21827-AJ Jordan/McAliley)-2012-03-07

Expert Witness for Plaintiffs - Intellectual Property Trademark Infringement - Deposition encompassing spoliation of electronically stored evidence when large data files were copied to a computer server after order was granted on motion to compel production of electronic data storage device for forensic examination, resulting in thousands of keyword search hits in unallocated space.

U.S. vs. Bradley A. Morales (U.S. Navy Southern Judicial Circuit, OCN:13JUN08-GCPF-0108-8BMA)-2009

Expert Witness for the Department of the Navy Defense - Marine Corps Recruit Depot, Parris Island - Testimony determining the origins of files and methods used to create those files existing on computer systems, external drives, and various media, recovering deleted data, the value of metadata information, and detailing how electronic information is stored and extracted from iPod devices.

Rivera and Abell vs. Bio-Engineered Supplements & Nutrition, Inc. (U.S. District Court Central District of California, Case No. 07-CV-01306-JVS-RNB)-2009

Expert Witness for Defendants - Fraud - Deposition on electronic discovery requests encompassing the processing and production of more than three-million emails, and identifying and limiting trademark secrets and privileged information from Microsoft Exchange servers across an organizations regional network.

Smith vs. Effective Teleservices, Inc., et al. (15th Judicial Circuit Palm Beach County, FL, Case No. 502005CA006080 Barkdull)-2008

Appointed Neutral Expert - Business Reorganization - Testimony determining if previous discovery requests were met and if spoliation of electronically stored information occurred on an email production of 2900 mailboxes from a Microsoft Exchange server.

U.S. vs. Carlos Seafood, Inc. (U.S. District Court Southern District of Florida, Miami, Case No. 07-CR-20898-AJ Jordan/Turnoff)-2008

Expert Witness for Defendants - Conspiracy to Defraud, Smuggling, Money Laundering - Testimony encompassing the processes and procedures of obtaining electronically stored evidence through subpoenas to Internet Service Providers (ISP), how electronically stored email can be searched and limited by various metadata fields across multiple systems and devices to identify attorney-client privileged information.

U.S. vs. Andrew W. Hamrick (U.S. Navy Southern Judicial Circuit, OCN:12Oct2007-GCPF-0167-8BNA)-2008

Expert Witness for the Department of the Navy Defense - Jacksonville Naval Air Station - Testimony determining the authenticity of electronically stored information on media, file dates, digital images, peer-to-peer network systems, how internet history, cache, and cookies store information, and how spyware and viruses infiltrate and execute on computer systems. Demonstrated that although the files in questions did exist, it was not the defendant that downloaded or reviewed those files. *A note from the Command Executive Officer of the Navy Legal Service Office stated: "We couldn't have done it without you & AN Hamrick owes you his future. I can't thank you enough for your professionalism and efforts in this matter."*

Smith vs. Effective Teleservices, Inc., et al. (15th Judicial Circuit Palm Beach County, FL, Case No. 502005CA006080 Crow)-2007
Appointed Neutral Expert - Business Reorganization - Testimony on creating proper scopes for discovery of electronically stored information on email systems, analyzing the email production of 2900 mailboxes from a Microsoft Exchange server, and the necessity to include unnamed custodians in the keyword search process.

U.S. vs. Orlansky, et al. (U.S. District Court Southern District of Florida, Miami, Case No. 03-CR-20951-AJ Jordan/Brown)-2006
Expert Witness for Defendants - Bank Fraud, Wire Fraud, Money Laundering - Testimony encompassing the use of internal computer systems, tracking and identifying the owners, versions, and authors of electronically stored information through document metadata across an organizations network.

U.S. vs. Eric B. Lobsinger (U.S. Navy Western Pacific Judicial Circuit, OCN:09DEC04-FEYK-0353-8BNA)-2006
Expert Witness for the Government, Department of the Navy, at the request of the Naval Criminal Investigative Service (NCIS) - Testimony encompassing the authenticity of digital images, artistic rendering, imaging morphing, and how custom screen savers are created.

State vs. Yona Rabinowitz (15th Judicial Circuit Palm Beach County, FL, Case No. 502003CF007225AXXXMB)-2004
Expert Witness for the Florida State Attorney's Office and Palm Beach County Sheriff's Office - Deposition countering the defenses' forensic examiner conclusions as to how the suspect never downloaded or possessed the files located on his computer. Detailing how Microsoft operating systems work, remote access, telnet service, user authentication and access, password requirements, wireless networks, trojans, viruses, and peer-to-peer networks. *A letter of commendation from the commander of the PBSO Special Investigations Unit stated: "Mr. Kleiman conducted his own examination of the evidence in the case and found numerous errors in the defenses expert's report. With Mr. Kleiman's assistance, a case that was destined to go to court was closed with the suspect pleading guilty a day before trial was to begin. Mr. Kleiman worked weeks reviewing evidence in this case and preparing report and never asked for compensation for his time and hard work."*

Publications / Certifications / Education / Speaking Engagements / Affiliations

Published works:

- Cisco Router and Switch Forensics: Analyzing Malicious Network Activity, Co-Author, ISBN: 978-1597494182, May 2009
- Overwriting Hard Drive Data: The Great Wiping Controversy, Co-Author, Lecture Notes in Computer Science, Dec 2008
- Perl Scripting for Windows Security: Technical Editor, ISBN: 978-1597491730, Jan 2008
- The Official CHFI Study Guide: (Exam 312-49), Lead Author and Technical Editor, ISBN: 978-159749197-6, Oct 2007
- Windows Forensic Analysis: Including DVD Toolkit, Technical Editor, ISBN: 978-1597491563, April 2007
- Rootkits for Dummies: Forensic Advisor, ISBN: 978-0471917106, Jan 2007
- CD and DVD Forensics: Technical Editor, ISBN: 978-1597491280, Nov 2006
- How to Cheat at Windows System Administration, Co-Author, ISBN: 978-1597491051, Sep 2006
- Enemy at the Water Cooler: Real Life Stories of Insider Threats, Technical Reviewer, ISBN: 978-1597491297, Aug 2006
- Winternals: Recovery and Administration Field Guide, Lead Author and Tech Editor, ISBN: 978-1597490795, Jun 2006
- Security Log Management: Identifying Patterns in the Chaos, Co-Author, ISBN: 978-1597490429, Jan 2006
- Perfect Passwords: Selection, Protection, Authentication, Technical Editor ISBN: 978-1597490412, Dec 2005
- Microsoft® Log Parser Toolkit: Investigating Intrusions, Co-Author, ISBN: 978-1932266528, Feb 2005

Certifications:

- Microsoft Windows Enterprise Security - Most Valuable Professional (**MVP®**)
- Information Systems Security Management Professional (**ISSMP®**)
- Information Systems Security Architecture Professional (**ISSAP®**)
- Certified Information Systems Security Professional (**CISSP®**)
- Certified Electronic Evidence Collection Specialist (**CEECS**)
- Certified Professional in Comprehensive Security (**CPCS**)
- Certified Information Forensics Investigator™ (**CIFI**)
- Certified Information Security Manager (**CISM®**)
- Microsoft Certified Systems Engineer (**MCSE®**)
- Digital Forensics Certified Practitioner (**DFCP**)
- Certified Anti-Terrorism Specialist (**CAS**)
- Certified Data Recovery Expert (**CDRE**)
- Certified Computer Examiner (**CCE®**)

Professional Affiliations:

- Member - Applications Committee - National Center for Forensic Science-Digital Forensics Certification Board (**DFCB**)
- Member - International Association of Computer Investigative Specialists® (**IACIS**)
- Member - International Society of Forensic Computer Examiners® (**ISFCE**)
- Member - International Information Systems Forensics Association (**IISFA**)
- Member - Information Systems Audit and Control Association® (**ISACA**)
- Member - Miami Electronic Crimes Task Force (**MECTF**)
- Member - Anti Terrorism Accreditation Board (**ATAB**)
- Member - High Tech Crime Consortium (**HTCC**)
- Member - FBI **InfraGard**

Speaking Engagements / Instructor Lead Training:

- Preliminary live preview with Log Parser and other Scripts Tools and Tricks – DFIROnline - <http://www.writeblocked.org/index.php/dfironline.html>, Online, Sep 2012
- Intro to Computer Forensics: How You Can Help Your Expert and Your Expert Can Help You - Annual NLSO Southeast/Central Command Training Mayport Naval Station, Jacksonville, FL, Sep 2009
- Scripting Network Forensics - Featuring: Powershell, Log Parser, Perl, Sysinternals, Guidance Software CEIC, May 2009
- Digital Forensics and the PI Laws: What is Happening and What You Can do to Help, Guidance Software CEIC May 2009
- Lose the Geek-Speak: Creating Client Friendly Forensic Reports, Guidance Software CEIC, May 2009
- Forensic Science and Law Summit - BrightTalk - Digital Forensics Private Investigation Laws, Dec 2008
- Digital Investigation Summit - BrightTalk - Digital Forensics: The DFCB and the ABA Resolution, Oct 2008
- Live Preview-Tools-Tricks-n-Traps/Log File Forensics, Sarasota FL, FACCI, 2008 Annual Training, Jul 2008
- Live Preview-Collecting Preliminary Evidence from Live Computer Systems, InfraGard Miami, Annual Meeting, June 2008
- Locating Intrusions and Collecting Evidence on Live Computer Systems, Palm Beach, FL, PBCGov, Sep 2007
- Log File Forensics Tools and Tricks, San Diego, CA, HTCIA International Training Conference, Aug 2007
- Tools, Tricks, and Traps: CyberCrime Institute, Kennesaw State University, GA, CyberCrime Summit, Mar 2007
- Florida Bar Approved CLE Course # 2569 6, West Palm Beach, FL, Effective e-Discovery, Jun 2006
- Advanced Log File Forensics: CyberCrime Institute, Kennesaw State University, GA, CyberCrime Summit, Mar 2006
- Forensic Incident Response through Log File Analysis: Tampa, FL, DoD Cyber Crime Conference, Jan 2006
- Forensics for Information Security Managers: Vienna, VA., (ISC)2, Sep 2005
- Following an Intrusion through a Microsoft® Network: Washington, D.C., FBI InfraGard National Conference, Aug 2005
- Secure Electronic Environments: Cleveland, OH, Nuclear Information Technology Strategic Leadership, Jun 2005
- Secure Document Delivery Concepts and Options: Ft. Lauderdale, FL, ISSA, Nova University, May 2005

Education:

- United States Army -1986-1990 Aviation Logistics: Distinguished Honor Graduate - Aviation duties, avionics, and encrypted communications - 1987 U.S. Army Soldier of the Year
- Indian River Community College - Ft. Pierce, FL -1992: Criminal Justice. (Distinguished Honor Graduate)
- Embry-Riddle Aeronautical University - FL - 1988 to 1989: Professional Aeronautics. (Dean's List)
- University of Maryland - 1987 to 1988: Computer Science.
- Palm Beach Community College - Palm Beach, FL - 1983 to 1986/1992: Computer Science, Criminal Justice. (Presidents Honor Roll)